PETER P. SWIRE*

Of Elephants, Mice, And Privacy: International Choice of Law and the Internet

> The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet.[1]

We are leaving one era and entering another. In the earlier, romantic era, the hope and belief was that geography would prove "a virtually meaningless construct on the Internet." In the newer more legalistic era,[2] geographic sovereigns are putting into place a large and rapidly expanding number of rules that target Internet behavior.[3] In the romantic era, there were brave declarations that "the Internet treats censorship as damage, and routes around it," or "national borders

*Peter P. Swire is a Professor at the Ohio State University College of Law. Professor Swire received his A.B. degree in 1980 from Princeton University and his J.D. from Yale University in 1985. Special thanks to Joel Reidenberg and Jane Winn for their roles in helping create the article, to David Post for pointing me to the *Pataki* quote, and to Sandy Caust-Ellenbogen and Art Greenbaum for comments. Fine research assistance was provided by Jennifer Larraguibel and Timothy McGranor. My thanks also for financial support for the research from an Ameritech Faculty Fellowship, the Brookings Institution, and the Ohio State University College of Law.

1. Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 168-69 (S.D.N.Y. 1997).

2. The word "era" was traditionally used to describe one of the five major divisions of geologic time. WEBSTER'S THIRD NEW INT'L DICTIONARY 769 (1986). In "Internet time," an era can last only a few years, perhaps less.

3. In one week in July 1998, the U.S. Senate considered legislation that would: (1) require filtering software on computers in schools and libraries that get federal funds for Internet hookups; (2) make it a crime for commercial websites to distribute or display to minors any material that could be "harmful" to children; (3) give the Federal Bureau of Investigation access to the customer records of Internet service providers in investigations of pedophilia without an order from a court or grand jury; and (4) make it criminal to gamble over the Internet. Jeri Clausing, *Senate's Internet Legislation Under Fire*, N.Y. TIMES, July 27, 1998, at D5.

aren't even speed bumps on the Information Superhighway.''[4] In the newer era, a CompuServe executive in Germany can be sentenced to jail for failing to filter out material objectionable to a Bavarian prosecutor.[5] And, as discussed in this article, the European Union (EU) might consider most commercial websites in the United States to be governed by its new privacy rules.[6]

For this symposium on *Jurisdiction and the Internet*, this article pursues three overlapping tasks. The first task is to go beyond jurisdiction by exploring choice of law issues. For many modern transactions, multiple sovereigns will have personal jurisdiction based on the significant activity within their borders. Consequently, even where jurisdiction exists, there is the additional important question of determining when a sovereign will impose its own rule, or instead choose to have the law of a different sovereign govern. In order to provide a baseline understanding of the subject, Part I presents an introduction to choice of law rules within the European Union (EU) and discusses the framework for choice of law in transactions involving both the European Union and the United States.

The second task of the article is to explore how choice of law rules will operate for an emerging area of law with important implications for the Internet. In October 1998, the European Union Directive on Data Protection (Data Protection Directive) entered into effect.[7] The discussion of this privacy Data Protection Directive will draw on research undertaken for a book entitled *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*.[8] Part II of this article provides an overview of the Directive. The Directive harmonizes, to an unprecedented extent, the laws regulating the use of personal data. Such harmonization offers one alternative to choice of law rules, for there is obviously no need to choose if all the rules are the same. On closer inspection, however, such harmonization is far from complete. The European Union has created elaborate and largely nonjudicial mechanisms for resolving the remaining problems. Part II analyzes the resultant choice of law regime. It also critiques proposals to understand this regime to expand EU jurisdiction to a vast range of websites in the United States and around the world. Part II

4. E-mail from Timothy C. May to the e-mail listserv, owner-cypherpunks@toad.com (Feb. 13, 1997) (on file with the author). E-mail from JohnYoung to the e-mail listserv, cypherpunks@toad.-com (Apr. 5, 1998) (on file with the author). For a leading academic expression of the romantic position, *see* David R. Johnson & David G. Post, *Law And Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

5. *Morning Briefcase*, DALLAS MORNING NEWS, May 29, 1998, at 2D (describing suspended two-year prison sentence received by the former head of CompuServe Corp's German unit for allowing distribution of pornography on the Internet through the company's network).

6. *See infra* notes 94 to 117.

7. Council Directive 95/46, 1995 O. J. (L281) 31 [hereinafter Directive 95/46], available *in* <http://europa.eu.int/comm/dg15/en>.

8. PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998) [hereinafter SWIRE & LITAN].

concludes by applying the choice of law rules of the Data Protection Directive and the EU Distance Selling Directive[9] to sample transactions.

The third task of the article is to explore more generally when and whether legal regulation of the Internet is likely to be effective. As a normative matter, dueling fears exist about over-regulation and under-regulation. The fear of over-regulation, expressed by the court in *Pataki*, is "that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed."[10] The contrary fear of under-regulation is that important social harms might take place over the Internet unless governments enforce strict laws prohibiting such behavior. In fact, as discussed in Part III, every sovereign has identified some actions over the Internet that it considers harmful enough to deserve regulation. Sovereigns differ enormously, however, in which actions they consider harmful. A related problem is that multiple sovereigns will often have jurisdiction over a potential defendant, and choice of law issues will inevitably arise in determining which sovereign's rules should apply in a given instance.

Part III suggests the metaphor of "elephants" and "mice" for understanding when legal regulation of the Internet is most likely to be effective. In brief, elephants are large organizations that have major operations in a country. Elephants are powerful and have a thick skin, but are impossible to hide. They are undoubtedly subject to a country's jurisdiction. Once legislation is enacted, they likely will have to comply. By contrast, mice are small and mobile actors, such as pornography sites or copyright violators, that can reopen immediately after being kicked off of a server or can move offshore. Mice breed annoyingly quickly—new sites can open at any time. Where harm over the Internet is caused by mice, hidden in crannies in the network, traditional legal enforcement is more difficult. In such instances legal enforcement, to be successful, will focus on someone other than the mice themselves. Candidates for enforcement include the individual users, the Internet service providers, the financial intermediaries that transfer money to the mice, and the offshore countries that provide the mice a cozy nest. By exploring the metaphor of the elephants and the mice, we develop a sense of how choice of law and legal regulation are likely to develop for the Internet.

I. Choice of Law in the European Union

The choice of law regime in the European Union is complex.[11] The goal in this article is to introduce some of the main components and begin to see how

9. Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in respect of Distance Contracts [hereinafter Distance Selling Directive], available *in* <http://europa.eu.int/comm/dg24/policy/developments/dist_sell/index_en.html>.

10. *Pataki*, 969 F. Supp. at 168-69.

11. *See generally* MATHIAS REIMANN, CONFLICT OF LAWS IN WESTERN EUROPE: A GUIDE THROUGH THE JUNGLE (1995) [hereinafter Reimann].

the rules apply to Internet transactions. The complexity results, in good measure, from the different levels of authority that purport to govern choice of law rules. Rules can be set at the national or even sub-national level, in bilateral agreements, as a matter of EU law, or in multilateral conventions. Quite often, the rules created in these various fora themselves conflict. Choice of law must clarify which of the apparently relevant rules govern in a particular context. In researching choice of law, the traditional starting place would be the national law of the sovereign whose court is hearing a dispute. For instance, an English court might first turn to English choice of law rules in addressing a contract or tort dispute. Over time, however, countries have entered into some important multilateral conventions to harmonize choice of law rules, such as the Rome Convention discussed below.[12] These conventions, once adopted by a country, typically take precedence over preexisting national choice of law rules.

In researching European choice of law, it is not enough to research only national rules and bilateral or multilateral agreements. As discussed in Part II, in connection with the Data Protection Directive, regulation by the European Union applies directly to the member states. Where the European Union acts through a Directive, the member states are required to enact implementing legislation. Choice of law rules in such legislation, which must comply with the Directive, take precedence over preexisting national law.

Amidst this complexity, there is a persistent drive for harmonization. Over time, the European Union has expanded from six original members to the present fifteen. The depth of economic and political integration has also steadily increased, culminating with both the political union embodied in the Treaty on European Union signed at Maastricht in 1992[13] and with the introduction of the Euro as a transnational currency. Continued harmonization of choice of law rules is a next logical step in the creation of Europe's unified internal market. The proliferation of international transactions involving the Internet will provide a further impetus for such harmonization.

A. The Rome Convention

A key document for harmonizing choice of laws in Europe is the European Community Convention on the Law Applicable to Contractual Obligations,[14] commonly known as the Rome Convention. The Rome Convention, by its terms, applies to "contractual obligations in any situation involving a choice between the laws of different countries."[15] In practice, important limitations exist on its

12. Convention on the Law Applicable to Contractual Obligations, 1980 O.J. (L 266) 1 [hereinafter Rome Convention]. *See generally* Richard Plender, The European Contracts Convention: The Rome Convention on the Choice of Law for Contracts (1991).

13. Treaty on European Union, 1992 O.J. (C224) 1, 1 C.M.L.R. 719 (1992), *reprinted in* 31 I.L.M. 247 (1992).

14. Rome Convention, *supra* note 12.

15. *Id.* art. 1(1).

general applicability. First, the Rome Convention does not take precedence over choice of law rules that are included in EU legislation.[16] The discussion below of the Data Protection Directive illustrates how EU law is often now the authoritative source for choice of law in many settings. Second, the Rome Convention does not apply where a member state has joined an international convention on a certain topic.[17] A prominent example, discussed below, is the United Nations Convention on Contracts for the International Sale of Goods,[18] which governs many sales of goods involving the United States and an EU Member State.[19] The convention also exempts from coverage certain substantive areas, including wills and succession,[20] domestic relations,[21] commercial paper,[22] corporate law,[23] and trusts.[24] These substantive areas, however, are mostly covered by other international agreements that help supply uniform choice of law rules.[25]

Contracting parties are generally free to designate whatever law they wish, even if it is the law of a country not bound by the Rome Convention.[26] Predictably, this broad principle has important limitations. For instance, parties cannot avoid the mandatory rules of a country if all parts of the contract are closely connected to that country.[27] Suppose a landlord rents an apartment to a tenant in England. Both parties live in England and the apartment is in England, but the lease provides that French law applies. In such a case, the tenant would benefit from any mandatory rules under English law, notwithstanding the usual Rome Convention principle of freedom of choice.[28]

Consumer contracts are another important exception to the freedom of contractual parties to choose the applicable law.[29] The consumer exception to the Rome Convention applies to a contract for goods or services (or a contract for credit

16. *Id.* art. 20.

17. *Id.* art. 21.

18. United Nations Convention on Contracts for the International Sale of Goods, 3 I.L.M. 668 (1980) [hereinafter CISG].

19. For a recent critique of the Rome Convention, *see* H. Matthew Horlacher, Note, *The Rome Convention and the German Paradigm: Forecasting the Demise of the European Convention on the Law Applicable to Contractual Obligations*, 27 CORNELL INT'L L.J. 173 (1994).

20. Rome Convention, *supra* note 12, art. 1(2)(b).

21. *Id.*

22. *Id.* art. 1(2)(c).

23. *Id.* art. 1(2)(e).

24. *Id.* art. 1(2)(g).

25. *See, e.g.*, The Geneva Convention on the Law Applicable to Bills of Exchange and Promissory Notes, June 7, 1930, 143 L.N.T.S. 257; The Geneva Convention on the Law Applicable to Cheques, Mar. 19, 1931, 143 L.N.T.S. 355.

26. Rome Convention, *supra* note 12, art. 2. The parties are also free to choose a law for a certain portion of the contract. *Id.* art. 3(1).

27. *Id.* art 3(3).

28. *Id.* art. 7(1).

29. *Id.* art. 5. For an excellent compilation of the way that European Union consumer law has effected French contract law, *see* Jerome Huet, *European Community Sources of French Contract Law*, 5 TUL. J. INT'L & COMP. L. 85, 86 (1997). For general discussion of European consumer law, *see* VIVIENNE KENDALL, EC CONSUMER LAW (1995).

for those goods or services) where the consumer acts as a private person outside of his or her "trade or profession."[30] In such cases, individuals will receive the protection offered consumers in the country of their habitual residence[31] provided that: (1) the contract was the result of advertising or an invitation of the person providing goods or services (vendor); (2) the vendor received the consumer's order in the consumer's country; or (3) the vendor arranged for the consumer to come to the vendor's country to complete the contract.[32] In other situations, the consumer transaction will still be governed by the Rome Convention. Consider, for instance, a consumer who lives in England, but buys property in France under a contract that calls for application of Belgian law. The consumer might expect to receive the protection of English law, if the contract were the result of advertising or one of the other listed criteria. English consumer laws would not apply, however, because the consumer exception applies to goods and services, but not to land. The general freedom-of-choice principle of the Rome Convention would dictate use of Belgian law.

Where the Rome Convention does apply, but there is no express choice-of-law provision, the court will look to see if the parties' implied choice has been "demonstrated with reasonable certainty."[33] If no choice can be implied with reasonable certainty, then the court will apply the law of the country with which the contract is most "closely connected."[34] A contract is presumed to be most closely connected: (1) to the country of residence of an individual effectuating performance, or (2) to the location of central administration for a business effectuating performance.[35] For example, where the contract contains no choice of law provision, and a company in England buys widgets from a company in France, French law will govern.[36] If the contract is for real property, then in the absence of a choice of law provision the law of the country where the property is located is presumed.[37] Any of these presumptions can be overridden if it appears, for whatever reason, that the contract is most closely connected with another country.[38]

B. The UN Convention on Contracts for the International Sale of Goods

Although the Rome Convention governs choice of law for contracts between Member States of the European Union, the United States is not a signatory.

30. Rome Convention, *supra* note 12, art. 5(1).
31. *Id.* art. 5(2).
32. *Id.*
33. *Id.* art. 3(1).
34. *Id.* art. 4(1).
35. *Id.* art. 4(2).
36. Note, however, that the outcome would be different if the widgets were bought for personal use and the consumer exception to the Rome Convention applied. In that situation, as discussed above, French law would be overridden by relevant, mandatory provisions of English consumer law. Rome Convention, *supra* note 12, art. 5.
37. *Id.* art. 4(3).
38. *Id.* art. 4(5).

However, many contracts involving Europe and the United States are governed by the UN Convention on Contracts for the International Sale of Goods (CISG),[39] which the United States has signed. By the terms of the Rome Convention, the CISG takes precedence when the two conflict.[40]

The CISG applies to contracting parties who have their places of business in different states, when both states are signatories of the CISG.[41] For instance, if a company in the United States agrees to buy widgets from a company in England, the CISG would govern the contract on whichever side of the Atlantic that suit was ultimately brought. At least in theory, the CISG provides significant stability in the law of international sales. The CISG goes beyond the choice-of-law approach of the Rome Convention and endeavors to supply substantive rules to govern a contract.[42]

The scope of the CISG, however, is limited in important respects. First, the CISG applies only to the sale of goods[43] and not to any contract as the Rome Convention does.[44] Second, the CISG contains a very large exclusion; it does not apply to sales of goods bought for "personal, family or household use," namely consumer goods.[45] Consumer contracts are typically governed by the choice of law provisions of the consumer's home country; in practice, this means that consumers also often receive the protections of their home country's substantive law. Next, the CISG does not apply to negotiable instruments, stocks, shares,[46] situations where the buyer is supplying a substantial amount of the parts necessary to make the good,[47] or situations where a substantial part of the contract is for services.[48] Nor does the CISG apply to any personal injury or death caused by the goods.[49] The CISG is not concerned with the validity of the contract or the title of the goods sold.[50] Finally, the CISG can be excluded from application by an agreement of the parties.[51]

39. CISG, *supra* note 18.

40. Rome Convention, *supra* note 12, art. 21.

41. CISG, *supra* note 18, art. 1(1). In the United States, it does not apply when one contracting party has its place of business in the U.S. and the other has its place of business in a non-signing state. Article 1(1)(b) states that the CISG would apply if the rules of private international law would lead to application of the signor state's law, but the United States has opted out of that provision in accordance with Article 95.

42. The preamble to the CISG states, "BEING OF THE OPINION that the adoption of uniform rules which govern contracts for the international sale of goods and take into account the different social, economic and legal systems would contribute to the removal of legal barriers in international trade and promote the development of international trade." CISG, *supra* note 18, at 671.

43. *Id.* art. 1(1).

44. Rome Convention, *supra* note 12, art. 1(1).

45. CISG, *supra* note 18, art. 2(a).

46. *Id.* art. 2(d).

47. *Id.* art. 3(1).

48. *Id.* art. 3(2).

49. *Id.* art. 5.

50. *Id.* art. 4.

51. *Id.* art. 6.

C. Choice of Law in Torts

Originally, the Rome Convention was meant to include noncontractual obligations as well as contractual ones.[52] Due to the influence of the United Kingdom, however, noncontractual obligations were dropped from its scope.[53] Individual countries have been left to set their own choice of law rules for torts. Conflicts are reduced because most of the countries of the European Union follow the same rule, that of *lex loci delicti*, or the law of the place where the tort was committed.[54] However, disagreements can arise, such as when the act and the harm occur in different places. For example, if a company in England puts up a website that defames a person in France, what law is to be applied? The answer will depend on the choice of law rule where the suit is brought because the countries of the European Union are split as to whether the place of the act or the place of the harm is used to determine the applicable law.[55]

II. The European Union Directive on Data Protection

The brief summary of European choice of law rules provides a sense of the incomplete harmonization in the current international regime for choice of laws. Specialized rules exist for different sorts of transactions. Even within the European Union, special choice of law rules often exist as provided by EU law.

Part II examines the EU Data Protection Directive, both as an example of a specialized choice of law regime and as new law that will apply to many Internet transactions. The Directive illustrates both the potential and the limitations of harmonization as a way to avoid choice of law problems. It also illustrates the leading role played by networks of administrative agencies, rather than judicial decisions, in the development of international choice of law.

A. Overview of the Directive

The European Union Data Protection Directive (Directive) was adopted in 1995 and took effect on October 25, 1998. The Directive is sweeping in scope, applying to all "processing" of "personal data," with only limited exceptions.[56] Processing is a broad term that means "any operation or set of operations which is performed upon personal data, whether or not by automatic means."[57] Personal

52. *The EEC Draft of a Convention on the Law Applicable to Contractual and Non-Contractual Obligations*, 21 Am. J. Comp. L. 584 (1973).

53. *See* Paul Lagarde, *The European Convention on the Law Applicable to Contractual Obligations: An Apologia*, 22 Va. J. Int'l L. 91, 92 (1981).

54. Reimann, *supra* note 11, at 135.

55. *Id.* For citations to U.S. discussion of digital defamation, *see* Michael Hadley, Note, *The Gertz Doctrine and Internet Defamation*, 84 Va. L. Rev. 477, 478 n.11 (1998).

56. Directive 95/46, *supra* note 7, arts. 2 & 3. *See generally* Swire & Litan, *supra* note 8, ch. 2.

57. Directive 95/46, *supra* note 7, art. 2(b).

data is a similarly broad term, meaning "any information relating to an identified or identifiable natural person ('data subject')."[58]

Pursuant to the Directive, each EU Member State must adopt a strict privacy law that provides clear rights to data subjects. When collecting information from an individual, those processing data (individuals known as the "controllers") must disclose their identities, their purposes for processing, and other information.[59] Data can only be processed for the announced purposes,[60] contrary to the common U.S. practice of permitting a company to use personal data for unlimited purposes. Before data can be provided to third parties for direct marketing, the individual must be informed and have the right to opt out free of charge.[61] Those processing personal data must guarantee that individuals have access to their own personal data and the opportunity to correct that data.[62] Other rules apply, such as special restrictions on the processing of sensitive data, including information about racial or ethnic origin, political opinions, or the processing of data concerning health or sex life.[63]

In considering enforcement of these rights, it is vital to recognize that the Directive does not itself apply to any behavior; instead, the Directive requires each EU Member State to promulgate a law that complies with the Directive's terms. Actual enforcement will thus take place under the law of a particular Member State.[64] Each country must establish one or more data protection agencies, known as "supervisory authorities," to help implement privacy rights. Supervisory authorities are required to have investigative powers, "effective powers of intervention," and the power to engage in legal proceedings or to bring violations to the attention of judicial authorities.[65]

In practice, supervisory authorities have usually worked informally with controllers when complaints are filed. In many instances, the controller explains why the practice in fact complies with applicable standards or else agrees to modify the objectionable practice. This non-litigation approach is likely to predominate under the Directive as well. Nonetheless, more formal sanctions have been and will be used under national laws, including ordering the erasure of data

58. *Id.* art. 2(a). The Directive does not, however, apply to processing of personal data "by a natural person in the course of a purely personal or household activity." *Id.* art. 3(2).

59. *See id.* art. 10.

60. *See id.* art. 6(1)(b).

61. *See id.* art. 14(b).

62. *See id.* art. 12.

63. *See id.* art. 8(1).

64. If a member state does not enact such a law, then a suit could ultimately be brought in the European Court of Justice to require such enactment.

65. *See* Directive 95/46, *supra* note 7, art. 28(3). The Directive gives examples of "effective powers of intervention," such as "delivering opinions before processing operations are carried out" and "ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions." *Id.*

and bans on transfers of data to jurisdictions with weak or nonexistent privacy laws.[66] In addition to administrative remedies, Member States are required to provide to every person the right to a judicial remedy for breach of privacy rights.[67] Article 25 of the Directive, governing transfers of data out of the European Union, has drawn special attention. Article 25 allows transfers to third countries (i.e., Non-Member States) only if the third country ensures an "adequate" level of protection.[68] Although the meaning of "adequacy" will only be clarified with time, many European officials believe that the United States lacks adequate protection, at least for some important sectors.

Where there is not adequate protection, flows of personal information from Europe to the United States would be permitted only under one of the derogations (exceptions) in article 26. One important exception is when the data subject has given consent unambiguously in advance of the transfer.[69] Another is where the transfer is necessary for the performance of a contract, such as providing the name and address for shipping a purchase into Europe.[70] A different type of exception is where a supervisory authority believes there are "adequate safeguards" of privacy, such as where the transfer takes place under a contract that ensures that European-style rules will apply in the third country.[71] Unless one of the derogations is satisfied, transfers of personal data are not permitted to countries that lack adequate privacy protection.[72]

B. The Level of Harmonization Under the Directive

The Directive is a major step toward harmonizing data protection law, both within the European Union and around the world. At the same time, as discussed here, there are significant constraints on the degree of harmonization. Because of these constraints, choice-of-law problems can easily arise under the Directive. By understanding the nature of these choice-of-law problems for flows of personal

66. *See* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 Iowa L. Rev. 471 (1995).

67. *See* Directive 95/46, *supra* note 7, art. 22.

68. Adequacy is assessed "in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country." *Id.* art. 25(2). For extensive analysis of the adequacy of protection in the United States, *see* Swire & Litan, *supra* note 8, ch. 2(a).

69. *See* Directive 95/46, *supra* note 7, art. 26(1)(a).

70. *See id.* art. 26(1)(b).

71. *See id.* art. 26(2). The contractual approach is discussed at length in Swire & Litan, *supra* note 8, chs. 3 & 8.

72. A principal task of the Swire & Litan book, *supra* note 8, is to explore the implications and policy aspects of the article 25 requirement of "adequacy" and the possible consequent limits on transfers of personal data out of the European Union.

data, more general insights will be gained about legal regulation of data flows on the Internet.

Before adoption of the Directive, European data protection laws had important areas of both similarity and dissimilarity. Privacy laws have spread gradually since 1970 when the German state of Hesse enacted the first data protection statute.[73] As Professor Fred Cate has discussed, European data protection laws generally have had four features:

> [T]ypically they apply to both public and private sectors; they apply to a wide range of activities, including data collection, storage, use, and dissemination; they impose affirmative obligations (often including registration with national authorities of anyone wishing to engage in any of these activities); and they have few, if any, sectoral limitations.[74]

By the early 1990s, a large fraction of EU members had adopted national legislation containing these features. Beyond the broad similarities, however, the national laws exhibited some notable differences. For instance, the French National Commission on Informatics and Freedoms, known as the CNIL for its French abbreviation, has powers that at least in theory are as sweeping as its title. Companies processing a wide range of personal information are expected to register their proposed data processing with the CNIL, and the agency has significant powers to deny the proposed processing. The CNIL not only has broad powers over data protection, but has separate subcommissions on freedom to work, research and statistics, local government, and technology and security.[75] On a quite different model, German data protection law assigns responsibility for data protection to both state and national officials. The Data Protection Commissioners at both levels are expected to play an important advisory role, mobilizing public support and urging private and public entities to be cautious in their uses of personal information. Other European national laws have fallen between the French "regulatory" data protection system and the German "advisory" system. Moreover, as of 1990, Italy, Greece, Spain, and other European nations had not yet promulgated a national data protection statute.

The terms of the Directive were drafted and debated during the early 1990s, and adopted formally in 1995. (As discussed in more detail elsewhere, this timing meant that the drafters paid little attention to special problems arising from the Internet.)[76] The Directive is designed to further the creation of a unified market in Europe.[77] It is intended to prevent the sort of dispute that erupted in the late 1980s, when France threatened to ban flows of personal information between Fiat's operations in France and those in Italy, which had no national data protection

73. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 32 (1997).

74. *Id.* at 32-33.

75. *Id. See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 182-239 (1989).

76. *See* SWIRE & LITAN, *supra* note 8, ch. 3.

77. *See* Directive 95/46, *supra* note 7, at 31-32 (findings (1) to (9)).

statute.[78] Under the Directive, all Member States are understood to have a strong level of protection of personal information. Thus, the general rule, subject to choice of law limitations discussed below, is that personal data can be sent or processed within the entire European Union on the same terms as within a Member State.

The Directive undoubtedly increases the level of harmonization within the European Union by requiring every Member State to create a data protection agency and implement detailed statutes. In some significant, but difficult to measure way, passage of the Directive has also put pressure on other countries to adopt similar legislation.[79] A wide range of countries with extensive trade relations with the European Union might be found to lack adequate protection of privacy and thus might encounter limits on the transfers of personal information. The last few years have seen data protection laws enacted or seriously considered in European countries outside of the European Union and in far-flung countries such as Argentina, Brazil, Canada, and New Zealand.[80] In conversations with persons knowledgeable about these developments, it is clear that the Directive has played a prominent role in encouraging such legislation. The possible finding of inadequate protection has also been used as an argument for enacting new privacy legislation in the United States.[81]

Although the Directive has led to significant convergence in data protection laws, harmonization is far from complete. Actual enforcement does not take place under the Directive itself. Instead, national laws are being enacted to implement the Directive.[82] These laws will differ in both large and small ways from each other. The level of enforcement effort will also undoubtedly vary by country, due both to differences in views about proper policy and differing levels of enforcement resources and experience. Two notable areas where differences are likely to develop involve sensitive data and authorization for transfers to countries outside of the European Union.

"Sensitive" data is defined in article 8 as "personal data revealing racial or

78. *See* Schwartz, *supra* note 66, at 491-92. In the particular dispute, Fiat-France eventually entered into a contract with Fiat-Italy, which required Fiat-Italy to offer the protection of French law to the information once it was transferred to Italy.

79. For an insightful discussion of convergence in data protection regimes, *see* Colin Bennett, *Convergence Revisited: Toward a Global Policy for the Protection of Personal Data, in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (Philip E. Agre & Marc Rotenberg eds., 1997).

80. *See Privacy and Human Rights* (visited Oct. 21, 1998) <http://www.gilc.org/privacy/survey>.

81. *See, e.g.*, Marc Rotenberg, Speech in Brussels, Belgium entitled *Privacy and the Citizen in the Digital Age: The Era of Political Action* (Oct. 17, 1996) ("Some believe that we need a privacy agency to address the concerns raised in Europe by the application of the data directive to North America. This is not correct. We need a privacy agency to answer the concerns of consumers in the United States."). A copy of this speech may be accessed at <http://epic.org/staff/rotenberg/speech_brussels_10_96.html>.

82. Data protection laws, decisions of data protection agencies, and a wide range of other legal and policy material relevant to the Directive will be collected at <http://www.privacyexchange.org>.

ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." The general provisions of article 8 are quite strict, banning all processing of sensitive data except in enumerated circumstances such as receiving "explicit consent" for processing from the individual.[83] Moreover, several provisions in article 8 allow the Member State to set even stricter rules. For instance, Member States can provide that even with "explicit consent" they will not allow processing of categories of sensitive data.[84]

The potential lack of harmonization on sensitive data may have more far-reaching implications than appear at first glance. The reason is that some sensitive data might be included in an enormous range of databases. For example, human resources records might easily include information about health insurance or trade-union membership. Credit card records and other payment information might reveal purchases of pharmaceuticals or other health-related purchases. Purchases from book stores, visits to web pages, or subscriptions to periodicals might reveal political opinions or religious affiliation. In all of these instances, a routine method for processing data, which otherwise complies with the Directive, might be subject to non-harmonized national laws that prohibit such processing. Organizations that design their systems for the ordinary case might not have an infrastructure in place to process sensitive data legally.[85]

Another potentially important area involving a lack of harmonization is article 26, which creates the derogations (exceptions) that permit transfers of personal information to countries that lack adequate protection. Article 26(1) creates six derogations that allow transfers, such as where the individual has given unambiguous consent or the transfer is necessary for the performance of a contract. These exceptions apply, however, "save where otherwise provided by domestic law governing particular cases."[86] The Member States thus retain the discretion to nullify or limit the important exceptions, which are being counted on by many organizations to permit transfers, after the Directive went into effect in October 1998.

For data that does not fit within the exceptions in article 26(1), transfers may be legal under article 26(2) where "adequate safeguards" exist and a Member State authorizes the transfer. Major efforts are currently underway to design

83. *See* Directive 95/46, *supra* note 7, art. 8(2)(a).

84. *Id.* Member states can also set special rules in areas such as: processing of data by a health professional; creation of additional exceptions for reasons of substantial public interest; release of data relating to "offences, criminal convictions or security measures"; processing of data relating to administrative sanctions or civil trials; and conditions under which a national identification number or any other identifier of general application may be processed. *See id.* arts. 8(3)-(7).

85. As of the fall of 1998, American Airline was under a data embargo in Sweden not to transfer sensitive airline reservation data to the United States, including health data (e.g., wheelchair for a passenger) or ethnic origin (e.g., kosher food or no pork for Muslims). SWIRE & LITAN, *supra* note 8, at 133.

86. *See* Directive 95/46, *supra* note 7, art. 26(1).

model contracts that would be considered "adequate safeguards."[87] Decisions about adequacy, however, are likely to be made at the national level.[88] Some nations may not provide for approvals at all under article 26(2). As national laws to implement the Directive are put into final form, other areas will also emerge that lack harmonization. One example is in the scope of the definition of "personal data" in article 2, and especially the meaning of "identifiable data." New research by Professors Joel Reidenberg and Paul Schwartz reveals a significant number of such differences, and more will emerge with time.[89]

C. The Directive's Regime for Choice of Law and Harmonization

In light of the significant lack of harmonization that persists under the Directive, it becomes important to study the mechanisms for resolving differences in EU national data protection laws. The Directive provides three procedural mechanisms to assist harmonization: (1) revision of the Directive, (2) the "Working Party" of national experts, (3) and the so-called "Comitology" process of voting at the EU level. After examining these mechanisms, the discussion will turn to the explicit choice of law regime in article 4 of the Directive. Careful attention will also be given to the claim, advanced by some European officials, that article 4 greatly expands the jurisdiction of EU members over many websites in the United States and around the world.

1. *Procedures for Harmonization*

To the extent national differences persist in EU data protection law, in violation of the goal of encouraging a unified internal market, one solution is revision of the Directive over time. Article 33 explicitly contemplates such a process. The Commission is required to report on the implementation of the Directive no later

87. The author is working with one such effort, headed by Dr. Alan Westin and the Center for Social and Legal Research. The use of model contracts is discussed at length in Swire & Litan, *supra* note 8, ch. 8. The Working Party and European officials generally have shown a greater willingness over time to consider a constructive role for the contractual approach. *Compare* Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *European Commission First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy* (visited June 26, 1997) <http://www.open.gov.uk/dpr/d5020en2.htm> (saying contractual approach should only "rarely" be used), *with* Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries* (visited Apr. 22, 1998) <http://www.open.gov.uk/dpr/500598pa.htm> (showing greater willingness to consider use of contracts, especially for large international networks and where the parties to the transactions have affiliates in Europe) [hereinafter Working Party].

88. It is possible that decisions about standard contractual clauses will be made at the EU level, as provided by article 26(4). *See* Directive 95/46, *supra* note 7, art. 26(4). Interviews with European officials suggest that such harmonization is unlikely to occur at the early stages of use of contractual provisions.

89. Telephone interview with Professor Joel R. Reidenberg (July 26, 1998). The Reidenberg and Schwartz research was prepared for Directorate Generale 15 of the European Commission, and the written version was not public as of press time. *See generally* <http://europa.eu.int/comm/dg15/en>.

than October 2001, along with suitable proposals for amendments if necessary. In particular, the Commission's report is supposed to examine potential application of the Directive to the data processing of sound and image data, which is outside the scope of the current Directive. In doing so, the Commission must take account "of developments in information technology and in the light of the state of progress in the information society."[90]

A major force for harmonization is likely to be the "Working Party on the Protection of Individuals with regard to the Processing of Personal Data" (Working Party), created by article 29. The Working Party is composed of a representative of the supervisory authority or authorities for each Member State, along with a representative of the Commission and a representative for any authority or authorities established for European Community institutions. The principal task of the Working Party is to render expert advice on matters arising under the Directive.[91]

Although its actions are entirely advisory, the Working Party is nonetheless likely to be influential on data protection issues. The Working Party has already issued a number of widely-read reports on specific topics.[92] Additionally, national data protection agencies may act in agreement with such reports, especially considering their participation in drafting such reports. As national laws are written, national legislators might also adopt the position of the Working Party, both out of deference for the members' expertise and because of the convenience of following recommendations agreed upon at the EU level.

For questions of determining adequacy, this advisory process is supplemented by a binding, or "Comitology" process set forth in article 31. Suppose that, in an enforcement proceeding in one country, there is a determination that the United States, or a sector in the United States, lacks adequate protection. This finding of inadequacy could then be appealed to the article 31 Committee. The Committee would be chaired by a representative of the European Commission, who would submit to the Committee a draft of measures to be taken. The Member States would then vote on the proposal in Committee according to a weighted system in which larger countries have a greater vote. The national representatives to this Committee would be political appointees, and not necessarily data protection officials. After the vote, the Commission would adopt measures that would apply immediately.[93]

---

90. *See* Directive 95/46, *supra* note 7, art. 33.

91. Specifically, the Working Party shall give the Commission an opinion on the level of protection in the Community and in third countries, give an opinion on codes of conduct drawn up at the Community level, and advise the Commission on any proposed amendment to the Directive. Its opinions and recommendations on specific matters are also forwarded to the Commission and to the Committee, described below, that is formed under article 31. *Id.* art. 31.

92. Many actions of the Working Party are posted at the web site of the Directorate General XV, at <http://europa.eu.int/comm/dg15/en>.

93. If the Commission's measures are not in accordance with the opinion of the Committee, the Commission shall defer application of the measures for three months. During that time, the Council of the EU, acting by qualified majority, may take a different decision. A slightly different procedure

2. *Article 4: Strict and Perhaps Trés Strict*

The Directive's rules for choice of law (and perhaps for jurisdiction) are laid out in article 4.[94] To date, there has not been any authoritative guidance on the interpretation of article 4. The views expressed here are based on my personal reading of the text of article 4, informed by conversations with knowledgeable officials, scholars, and others.

The interpretation of article 4 begins with two terms of art. The first term is the "controller," which means the person "which alone or jointly with others determines the purposes and means of the processing of personal data."[95] The second term is a "processor," which means a natural or legal person "which processes personal data on behalf of the controller."[96] To get a sense of how the two terms operate, imagine a bank that contracts out the handing of certain back-office operations to a data processing company. The bank would be the controller, because it is in charge and determines the purposes of the data processing. The outside contractor would be a mere processor under the Directive and would act on behalf of the controller.

The basic rule under article 4 is that each Member State shall apply its own data protection laws where "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State."[97] Under this language, French law would apply to a controller established on French territory. By contrast, French law would apparently not apply to a

---

applies for situations under article 26(2), where a Member State authorizes a contract or other safeguard as adequate for transfer to a country that otherwise lacks adequate protection. Member States are required to inform the Commission and the other Member States of authorizations they grant under article 26(2). *See* Directive 95/46, *supra* note 7, art. 26(2). If a Member State or the Commission objects on justified grounds, the Commission shall take appropriate measures under the Comitology process just described. *Id.*

94. The rules for choice of law provide:

> 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
> (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
> (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
> 2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

Id. art. 4.

95. *Id.* art. 2(d).

96. *Id.* art. 2(e).

97. *See id.* art. 4(1)(a).

processor established on French territory if the controller were established in another Member State.

Things get trickier when the same controller is established on the territory of several Member States, such as where one company has operations throughout the European Union. In such cases, the rule appears to be that of the narrowest funnel—the controller must apparently comply with the strictest of the various laws that might be applicable. In the language of the Directive, the controller "must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable."[98]

These intra-European Union situations are straightforward, however, compared with the problems that can arise where the controller is in a third country, that is, outside of the European Union. The Directive provides that a Member State shall apply its own law where "the controller is not established on Community territory and, for purposes of processing personal data *makes use of equipment*, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."[99] This language has potentially sweeping implications concerning choice of law and jurisdiction, especially for websites in the United States and around the world. It raises difficult interpretive issues concerning the meaning of "makes use of equipment." An intriguing wrinkle is that the "makes use of equipment" language may have a significantly different meaning in the French and some other language versions of the Directive.

A straightforward reading of the text creates a choice of law rule that a Member State's law will apply wherever: (1) the controller is not established on Community territory, and (2) the controller makes use of equipment in the Member State (for more than mere transit). On this reading, article 4 does not alter a country's jurisdiction. If there is otherwise jurisdiction over the distant controller, and an action is brought in an EU state, then article 4 provides the choice of law rule. For reasons that will become apparent, I believe this to be an appropriate interpretation of article 4.

A more ambitious, and legally questionable, reading of article 4 would find that it speaks not only to choice of law, but to personal jurisdiction as well. To see this point, posit a backdrop of existing jurisprudence for personal jurisdiction in France, England, and other EU nations. Next, posit the existence of websites in the United States and elsewhere in the world that would not be subjected to European jurisdiction under the existing jurisprudence. Such websites are likely

98. *Id.* A different interpretation, raised in some conversations with European officials, would stress the singular in the term "national law applicable." Under this alternative interpretation, there would apparently be only one applicable law. The choice of law task would then be to determine the unique applicable law that applies. If this interpretation were adopted, then the Directive would require a potentially substantial new jurisprudence of how to select that unique law in the huge range of circumstances to which the Directive applies.

99. *Id.* art. 4(1)(c) (emphasis added).

to be extremely numerous, likely including operations that have no assets in Europe and that make no targeted solicitation to European customers. Indeed, others have highlighted the limits on jurisdiction over foreign sites even under the unusually sweeping jurisdiction jurisprudence of the United States.[100]

The surprising nature of the claim that article 4 expands the jurisdiction of European data protection law is clear. As just discussed, there would apparently be a category of U.S. websites that would not ordinarily come under the jurisdiction of European law. Now, however, under article 4 of the Data Protection Directive and implementing legislation in the Member States, these sites would suddenly be brought within the jurisdiction of European law for their data processing activities. This substantial expansion of the reach of EU law would not have taken place through a publicized or negotiated effort to expand jurisdiction law generally. Instead, the expansion would have taken place in a provision of a specialized Directive, without any mention of the term jurisdiction. Furthermore, the expansion of personal jurisdiction to websites around the world would take place through a Directive drafted in the early 1990s, before there was any significant deliberation about the nature of the Internet or how to regulate it.[101]

This jurisdiction-enhancing view of article 4 is no idle fancy. In an August 1998 meeting, a well-informed EU official answered a question concerning the application of the Directive to U.S. websites. The topic is apparently the subject of ongoing discussion among data protection officials, and may be the subject of a forthcoming Working Party paper. The official specifically mentioned article 4, stating: "[t]he general feeling is that the Directive would apply, especially in situations where the data are actively collected by the site."[102] Depending on the meaning of "actively collected," such a view might readily sweep most commercial U.S. websites into the reach of the Directive.[103]

Assessing the merit of the jurisdiction-enhancing view in part depends on the definition of when a controller "for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of said Mem-

100. Jack Goldsmith, *What Internet Gambling Legislation Teaches about Internet Regulation*, 32 INT'L LAW. 1115 (1998); Allan R. Stein, *The Unexceptional Problem of Jurisdiction in Cyberspace*, 32 INT'L LAW. 1167 (1998).

101. To date, interviews with European officials have not revealed any legal basis, outside of the text of article 4 itself, for claiming that the Directive expands the jurisdiction otherwise applying to websites or other controllers established outside of the EU. That is, there has been no mention of any other authority in European Union law that would authorize such a result.

102. The statement was made on condition that the speaker not be identified.

103. The European official did not define what was meant by "active collection" of data. It seems quite possible, though, that the use of cookies, which are used by many U.S. web sites, would count as "active collection." Cookies are pieces of code that web sites can send to a user's hard drive. They can be used to help the site collect and collate personal information about the user. *See* <http://www.junkbusters.com> (discussing "How Web Servers' Cookies Threaten Your Privacy"). Under the argument that article 4 expands EU jurisdiction, if cookies were to be considered "active collection" of data, then many or most U.S. commercial websites would be included within the scope of the Directive.

ber State." Consider a possible interpretation that is consistent with the plain English of the text and avoids the jurisdiction-expanding view discussed above. Under this interpretation, the provision would apply whenever the controller has equipment situated in the territory of the Member State. On this view, if controllers or their agents own or lease equipment in France, then French data protection law would apply. Such equipment could include items used by employees or agents in their French offices or during business trips to the country. Equipment used by processors, on behalf of controllers, could also qualify. By contrast, article 4 would not apply simply because a French resident surfed to a U.S. website. In such an instance, the controller may have no prior contact with France and so would not have "made use of equipment" in France.

This possible interpretation mentioned the "plain English of the text." The "plain French" is potentially significantly different. Rather than mentioning "makes use of equipment," the French text would apply national law wherever the controller has recourse "a des moyens" ("to any means") situated in the territory of the Member State.[104] The German and Italian versions may be more similar to the French than the English version.[105] The French version is echoed by the English version of recital twenty preceding the Directive, which states that "the processing should be governed by the law of the Member State in which the means used are located."

Under the French text, there is a stronger argument that article 4 applies to the U.S. website. A controller would have recourse "to any means" in France when the French individual uses the Internet. As argued by French and other data protection officials, these "means" could include the French individual's computer and the French telecommunications system that sends data from France to the U.S. website.[106]

Although the French text provides some support for the jurisdiction-enhancing view, a legal question exists as to whether, as a matter of EU law, a directive can order the member states to expand the reach of their jurisdiction. In other words, is it within EU competence to require expansion of jurisdiction? To date, officials personally interviewed by the author have not identified any legal basis for the view that a directive can do so.

---

104. The French text of article 4(1)(c) applies the law of the member state where: "c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, á des fins de traitement de donnés á caractére personnel, á des moyens, automatisés ou non, situés sur le territoire dudit Etat membre, sauf si ces moyens ne sont utilisés qu'á des fins de transit sur le territoire de la Communauté." For the full French text of the Directive, *see* <http://www2.echo.lu/legal/fr/dataprot/directiv/direct.html>.

105. E-mail from Giusella Finocchiar to CyberProf@mail.law.utexas.edu (Jan. 22, 1998) (on file with author). E-mail from Joel Reidenberg to CyberProf@mail.law.utexas.edu (Jan. 21, 1998) (on file with the auhor). The Italian version discusses the "strumenti" available in the member state, which perhaps falls between the English "equipment" and the French "moyens" (means). *See* <http://www2.echo.lu/legal/it/datipers/direttiv/direttiv.html>.

106. This position was taken by French and other officials who discussed the meaning of the Directive with me "on background" during the course of researching SWIRE & LITAN, *supra* note 8.

Even if it is legally permissible for a directive to require expansion of jurisdiction, the next question is whether article 4 creates such a requirement. There are multiple and weighty arguments against a jurisdiction-enhancing view that relies on the French text. First, as a formal matter, both English and French are official languages of the European Union, so there is no basis for claiming that the French text is privileged over the English text. Second, the French text can be sensibly interpreted in the way suggested here for the English text. The French text states that the controller must have recourse to any means in the Member State. If the controller has done nothing to control anything in France, and quite possibly does not even know a user is coming from France, then the controller may not have played an active enough role over any means in France to fit within the definition. Third, even if a U.S. website were to fit within the definition, article 4 quite possibly should be considered as a choice-of-law provision rather than a jurisdiction-enhancing provision. In other words, article 4 would be read to say that French law would apply if, and only if, personal jurisdiction exists over the website based on ordinary principles of jurisdiction law.

Finally, as a policy matter, there are serious concerns about greatly expanding personal jurisdiction through article 4. Objections were mentioned about the adoption process of article 4, namely the absence of a publicized debate to broadly expand jurisdiction law, the inclusion of major reforms in a specialized Directive without any mention of the term jurisdiction, and the major implications for legal regulation of the Internet even though the Internet was not considered in any significant way in the deliberations leading up to article 4. Additional objections to broad expansion of jurisdiction are familiar. There are traditional concerns about notice, fairness, comity, and national sovereignty in expanding the reach of European law to websites around the world. Stated differently, the jurisdiction-enhancing interpretation of article 4 would have major extraterritorial effects. Websites and others outside of Europe, who may not have taken any action to seek business from European customers, would be expected to conform their actions to the laws of distant countries.[107]

3. *Purchases in Person under Article 4*

Analysis of some examples will help make the rules of article 4 more understandable. The first example is a credit card purchase in person. Assume the following:

(1) the consumer is a French national living in France;
(2) the customer buys an item in Italy while on vacation; and
(3) the operations center for the credit card issuer is in England.

107. Even if judgments were not enforceable against website operators in the U.S., the individual operators may be at risk of enforcement if they ever travel to Europe for business or on vacation, a far-from-rare occurrence in this day and age.

Under article 4, the first task is to identify the controller or controllers who "alone or jointly with others determines the purposes and means of the processing of personal data."[108] The first controller is the retailer in Italy. That retailer is presumably established in Italy and would come under Italian data protection law.[109] If the retailer is established in the territory of several Member States (such as a Pan-European chain of stores), then necessary measures must be taken to ensure that each of these establishments complies with the obligations laid down by the applicable national law.[110] For instance, the retailer might have its headquarters and processing center in Germany. In such a case, the "narrowest funnel" rule means that the retailer must apparently comply with both Italian and German law for data arising from this transaction. By contrast, if an Italian retailer contracts for a German company to process the data, only the Italian law would apply. The German contractor would only be a processor and not a controller, so article 4 would not call for application of German law.

A second controller is the credit card company with its headquarters and operations center in England. This credit card company receives a great deal of personal information concerning transactions, and is a controller when it "determines the purposes and means of the processing"[111] of such data. Because the company is established in England, English data protection law would apply.

Notably absent in the analysis thus far is any role for French data protection law with regards to this French consumer. Although French data protection law would not appear to apply to this transaction,[112] it is possible that other consumer protection laws would apply. For instance, the credit card company would likely have to comply with consumer laws concerning topics such as interest rate disclosure.[113]

Next consider a variation on this first example:

(1) the consumer is a French national living in France;

(2) the customer buys an item in Italy while on vacation;

(3) the operations center for the credit card issuer is in England; and

(4) the credit card company stores its English records in a mainframe in the United States.

---

108. Directive 95/46, *supra* note 7, art. 2(d).

109. "Each Member State shall apply the national provisions . . . where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State." *Id.* art. (4)(1)(a).

110. *Id.*

111. *Id.* art. 2(d).

112. French law may apply in the billing process, if there is any entity established in France that qualifies as a controller.

113. One wrinkle could make the analysis even more complicated. Suppose the consumer in Italy purchased health-related products such as pharmaceuticals. Such a purchase would involve "sensitive" data under article 8 and, as discussed above, member states retain the right to promulgate especially strict rules for sensitive data. If Italy promulgated such rules for health-related data, it might be illegal to transfer information about the transaction to England and France, or might require special consent by the customer.

In this variation, the question is whether data can lawfully be transferred to the United States.[114] In brief, transfer is permitted if the United States or the credit card sector in the United States is found to have "adequate" protection of privacy.[115] If not, then the credit card company must fit within one of the derogations in article 26. In this example, the company could get unambiguous consent in advance from the consumer, probably including a notice that personal information may be sent to countries that lack adequate protection of privacy.[116] In the alternative, the credit card company in the United States could sign a contract with the company in England, agreeing that the data in the United States would be processed according to English data protection law. Transfers under the contract would be lawful, if the English Data Protection Registrar approved the contract.[117]

4. *Distance Selling under Article 4*

The second example suggests some different legal issues that arise when the consumer buys at a distance from the seller whether by mail-order, telephone, or over the Internet. Assume the following:

(1) the consumer is a French national living in France; and

(2) the seller is in Spain.

The seller is a controller who is established in Spain. The obvious law that applies here is Spanish data protection law. The question is to define the point at which the seller is also established in France, triggering French data protection law. For instance, there may be a telemarketer perched a mile inside Spain, whose entire business is making sales calls into France. Recital nineteen to the Directive provides modest guidance to the meaning of "establishment," stating that "the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect."[118] This language suggests that the Spanish telemarketer may not be established in France. On the other hand, in the course of delivering goods and services to French customers, the telemarketer may take actions that "establish" it in France. If so, then both French and Spanish data protection law would apply.

114. This question is considered at length in SWIRE & LITAN, *supra* note 8.

115. Directive 95/46, *supra* note 7, art. 25.

116. *Id.* art. 26(1).

117. *Id.* art. 26(2).

118. The full text of Recital 19 states:

> Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfills the obligations imposed by the national law applicable to its activities.

A variation on the example is as follows:

(1) the consumer is a French national living in France; and

(2) the seller is in the United States.

This scenario is the one discussed at length above in connection with the possible jurisdiction-enhancing effects of the Directive. If the controller is "established" in France, then French data protection law would apply. If the controller is not "established" in France, but comes under France's jurisdiction under usual jurisdictional principles, then French data protection law would once again likely apply. In such situations, where there is French jurisdiction, and the controller "makes use of equipment" in France, then article 4 states that French data protection rules shall apply.

The more controversial cases arise where the controller is not established in France, and where territorial jurisdiction would not exist under usual jurisdictional principles. In such circumstances, it is argued that article 4 should not apply, but some European officials have claimed that article 4 itself grants jurisdiction. It is possible that this dispute will ultimately be the subject of diplomatic discussions between the European Union and other countries as part of a broader dialogue about the scope of jurisdiction as applied to Internet transactions.

Apart from data protection law, the use of distance selling may trigger an entirely different set of compliance issues for sellers. The European Union has adopted a Distance Selling Directive that becomes effective on May 20, 2000.[119] The Distance Selling Directive applies to organized sales efforts that use a means of distance communication, including telephone, mail-order, or webpage.[120] Despite its wide application to Web sales and other distance selling, the Distance Selling Directive has received very little attention to date.[121] Perhaps most important to electronic commerce, the Distance Selling Directive grants the consumer the right to withdraw from a distance contract for at least seven working days without giving any reason and without penalty except for the cost of returning the goods.[122] Although there are significant exceptions to this right of withdrawal, a great many Web and other distance selling purchases are apparently covered.[123] The Distance Selling Directive also has its own choice of law provision. After

119. Distance Selling Directive, *supra* note 9, art. 15.

120. The definitions of "distance contract" and "means of distance communication" are defined in Distance Selling Directive, *supra* note 9, arts. 2(1) & 2(4). The covered means of communication are listed in Annex I.

121. A LEXIS search in August 1998 revealed no law review articles that had cited the Distance Selling Directive since its passage in 1997, and only three articles that mentioned it as a proposed Directive.

122. Distance Selling Directive, *supra* note 9, art. 6(1).

123. Exceptions to the right of withdrawal include: goods which, by reason of their nature, cannot be returned; unsealed audio or video recordings or computer software; and newspapers, periodicals, and magazines. *Id.* art. 6(3). In addition, the Distance Selling Directive excludes categories of sales including: financial services; goods sold at auction; immovable property; and to a limited degree, foodstuffs. *Id.* art. 3.

stating that the consumer may not waive the rights conferred under the Distance Selling Directive,[124] it provides:

> Member States shall take the measures needed to ensure that the consumer does not lose the protection granted by this Directive by virtue of the choice of the law of a non-member country as the law applicable to the contract if the latter has close connection with the territory of one or more of the Member States.[125]

In other words, EU consumers would apparently be offered the protection of their home-country law, notwithstanding efforts by the seller to have a contract that specifies the use of American or other non-EU law.

D. Concluding Thoughts on the Directive and Choice of Law

The discussion of the Data Protection Directive highlights two themes for the understanding of choice of law and the Internet: the uses and limits of harmonization, and the leading role of transgovernmental regulatory networks rather than courts.

The use of harmonization, which EU law sometimes refers to as "approximation,"[126] is an important and obvious way to reduce conflicts among national laws. Because so many modern transactions have a transnational component, such harmonization can help satisfy the desire for simplicity and certainty in commercial law. The Internet makes it increasingly easy and less expensive to contact sellers in distant lands, making the advantages of harmonization even more apparent.

Analysis of the Data Protection Directive, however, suggests some of the limits of harmonization. As a practical matter, even within the European Union with a Directive that expresses agreement on the basic rights to be protected, there are multiple and important areas where national laws can differ. Part of the variation might be explained by the ordinary political process of countries preserving the power to legislate on issues they consider important. Part of the variation, however, arises from the fundamental principles that are called federalism in the United States and subsidiarity in the European Union. Resolving issues at a more local level has benefits, including the democratic advantages of local control, the flexibility to adapt to local conditions, and the ability to experiment with different solutions to common problems. Given the important and enduring values of federalism and subsidiarity, there are inherent limits on the degree of harmonization. In a world where multiple sovereigns will often have territorial jurisdiction over a transaction, choice of law issues will remain inevitable and even common.

A second theme from the analysis of the Data Protection Directive is the small role played by the courts in its choice of law issues and the large role played by

124. *See id.* art. 12(1).
125. *Id.* art. 12(2).
126. *Id.* art. 1.

what Professor Anne-Marie Slaughter calls "transgovernmental networks."[127] Applied to privacy, this network describes the substantial interactions among the privacy agencies in the fifteen European Union countries, together with interactions among privacy officials, advocacy groups, regulated organizations, academics, and others around the world.[128] Professor Slaughter's research emphasizes the leading role played by regulators who have the same functional responsibilities in different countries.

The choice of law regime of the Data Protection Directive reflects the primacy of this sort of transgovernmental network. The Directive and its choice of law rules were initially drafted and negotiated with large input from the privacy agencies, but with little or no participation by courts. Over time, as discussed previously,[129] the Working Party of privacy commissioners has played a leading role in interpreting the Data Protection Directive. Under the Directive, national decisions about the adequacy of privacy protection will be appealed to the article 31 committee, where votes are taken by political representatives of the Member States. The European Court of Justice will not decide what countries have "adequate" protection.

More broadly, Professor Patrick Borchers has documented the considerably smaller role European courts play in jurisdictional issues as compared with U.S. courts.[130] For privacy and electronic commerce, many choice of law disputes may be resolved primarily within transgovernmental administrative networks rather than courts. In the future, the international banking and securities regulators, privacy regulators, or other regulators may agree among themselves which country will take the lead in regulating particular sorts of transactions. The formal and informal decisions within these networks may often deserve closer scrutiny by those seeking to understand the choice of law regime rather than the occasional choice of law decision by the courts.

III. Elephants, Mice, and the Legal Regulation of the Internet

Part II of this article discussed choice of law under the EU Data Protection Directive and showed how European privacy laws might apply to a wide range of transactions on the Internet, even for websites in the United States that do not seek European customers. This concluding part of the article addresses the more

127. Anne-Marie Slaughter, *The Real New World Order*, FOREIGN AFF., Sept.-Oct. 1997, at 183, 195. *See also* ABRAM CHAYES & ANTONIA H. CHAYES, THE NEW SOVEREIGNTY (1995).

128. I am currently involved in research, sponsored by the Berkman Center for Law and the Internet of the Harvard Law School, concerning the transgovernmental network of privacy agencies.

129. Working Party, *supra* note 87.

130. Patrick J. Borchers, *Comparing Personal Jurisdiction in the United States and the European Community: Lessons for American Reform*, 40 AM. J. COMP. L. 121 (1992). Borchers finds the European approach, based more on practical decisions about jurisdiction in specific areas, generally preferable to the American approach, which he characterizes as based too much on judicial theories of jurisdiction that are applied with little regard for specific context. *Id.*

general question of when law is likely to be effective for Internet activity. A critical change for the Internet will be the increase in situations where individuals engage in international transactions themselves, rather than through import-export companies or other intermediaries. As individuals themselves act internationally, the overall style of legal regulation will differ substantially for "elephants" and "mice." As one consequence, choice of law rules will be important with respect to the former but not the latter.

A. The Rise of International Sales to Individuals

In researching the book about the Data Protection Directive, one theme emerged about what is critically different legal regulation of the Internet—far more than before, individuals will routinely buy across national borders. To a surprising extent, direct marketing currently has had only a small international component.[131] True, transnational marketing has been more important for certain sectors, such as travel services and some very high-end products. But the dominant reality until now has been that individuals (except in border regions) quite rarely buy directly from a seller in another country.

This lack of international sales to consumers has been accompanied by an enormous growth overall in the level of international trade. Until now, international trade has overwhelmingly featured business-to-business transactions. Goods and services have generally been imported by businesses, and the ultimate sale to individuals has been made by companies licensed to do business in the consumer's country. Business-to-business sales will continue to increase rapidly in the emerging world of electronic commerce. Indeed, in purely financial terms, business-to-business sales over the Internet are much larger today than business-to-individual sales, and this predominance will continue in the future.[132]

Although business-to-business sales over the Internet are and will remain a larger portion of Internet sales, the greatest legal and policy ferment will occur for business-to-individual transactions. An important reason for this is that for business-to-business sales there are existing commercial practices in place, including bills of lading, letters of credit, and other accepted tools of international transactions. International banks and other intermediaries are experienced at facilitating international trade. When disputes arise, businesses can appeal to national laws and to a well-established system of commercial arbitration. In terms of choice of law, business-to-business sales are largely governed by the law selected by the parties under the authority of the Rome Convention, the United Nations Convention on the Law Applicable to the International Sale of Goods, and established legal precedents.

131. Swire & Litan, *supra* note 8, ch. 7.
132. *Id.* ch. 4.

The situation changes substantially when a business sells to individual consumers across national borders. European and American law often treat consumer contracts differently from business-to-business contracts. In general, consumers are not as able as businesses to waive their legal rights because of public policy concerns about adhesion contracts and the unfair bargaining power of the seller. As shown by both the Distance Selling Directive and the Data Protection Directive, consumer contracts are more likely to be subject to mandatory rules in the consumer's jurisdiction, making it more difficult for the contract to specify alternative choices of law. When disputes arise, there is no significant history of international arbitration of a consumer's dispute with a merchant. If disputes go to court, the process may be lengthy and expensive, and there is no certainty that the judgment of one country (such as the consumer's) will be enforced in the other country (such as the seller's).

In addition to these contract interpretation issues, other legal and policy problems multiply when international transactions are done with individuals rather than businesses. Existing problems often become more acute and enforcement far more difficult when international transactions involve millions of individuals rather than thousands of businesses. Consider the sorts of social harms that are likely to become more prominent as the Internet expands the ability of individuals to access websites and conduct transactions in other countries. Individual countries will vary on which items on the list they consider to be social harms, but every country has enacted laws forbidding at least some of the items listed below.

1. *Privacy and Data Protection*

The Internet creates the possibility of websites outside of Europe that can process personal information about individuals in Europe. If there are no limits on transfers of data to these sites, then data havens might develop outside of Europe, filled with personal data about European citizens in violation of the goals of the Data Protection Directive.

2. *Consumer Protection Laws Generally*

The Distance Selling Directive is one of many examples of a special legal regime for consumer protection. Countries now have a host of other consumer protection laws, covering topics such as: anti-fraud; proper advertising; usury limits; regulation of installment contracts, rebates, and other specific selling practices; and many more. There will be a growing demand to enforce these sorts of laws internationally as more consumers do business on the Internet. Enforcement will be especially difficult when the buyer and seller are not aware of each other's nationality. Problems will also arise when the site sells downloadable goods such as software, music, or information. In such instances, there are no parties involved in physical shipment of the goods who are ready targets for regulation.

3. *Professional Licensing*

The Internet makes it far easier for an individual to purchase professional services across borders. Examples might include legal advice, medical advice, psychological counseling, and sales of financial services. Jurisdictions may find it increasingly difficult to prevent outside persons from offering services without a license.

4. *Labor Laws*

Similarly, the Internet makes it easier for employers to hire individuals in distant countries, either full-time or on a contract basis. This sort of employment might raise difficult legal issues both in the employer's country (e.g., laws against hiring nonunion employees) and in the employee's country (e.g., laws that protect employees, such as anti-discrimination and minimum wage laws).

5. *Intellectual Property*

As copying of valuable information becomes easier, for both small corporations and individuals, the difficulty mounts for owners of intellectual property who wish to control dissemination of that information. By contrast, owners of intellectual property often can enforce more effectively where the purchasers are large corporations. One reason for easier enforcement is the risk that a disgruntled employee will blow the whistle on an employer's large-scale violation of copyright or other rules, at substantial expense to the employer.

6. *Taxation*

Today, international tax enforcement can focus on the relatively limited number of businesses that engage in importing and exporting. In the future, over the Internet, tax authorities fear they will not have any similarly effective way to track international transactions involving a much larger number of sellers and individual buyers.

7. *Gambling*

Countries vary widely in their approval of Internet gambling. It may be very difficult for the anti-gambling countries to prevent their residents from gambling at a site located in a country where the activity is legal.

8. *Pornography*

The Internet allows individuals around the world to access pornography, including child pornography, that is forbidden in the individuals' home country. Countries that wish to restrict pornography will face great challenges in preventing their residents from viewing material that is lawful in the country hosting the site.

9. *Hate Speech*

Some countries, such as Germany, have strict rules forbidding certain forms of hate speech, including Nazi propaganda. Such laws become much more difficult to enforce if free speech protections in other countries allow posting of Nazi or other material to the Internet.

10. *Treasonable or Other Politically-Censored Speech*

Some countries, such as Singapore and China, have laws forbidding certain sorts of political speech. The Internet makes it more difficult for countries to exclude such speech.

11. *Digital Defamation*

On the Internet, everyone can be a publisher. It becomes easy and cheap to have a webpage that can be accessed from around the world. Some of these webpages, perhaps many, contain malicious and untrue statements. Countries will vary in what must be proved to establish a claim for defamation.

This list suggests the perplexing array of harms that might occur as individuals gain the ability to visit websites from around the world. For many of these issues, we can expect major disagreements among national legal regimes. A central issue then becomes the extent to which a nation (or group of nations) can act effectively to protect against the harms that it considers important.

B. Elephants and Mice

In considering legal regulation of the Internet, there is an important distinction between large players, which one might call "elephants," and small, mobile actors called "mice." The style of regulation against elephants and mice differs substantially. Elephants are large, powerful, and practically impossible to hide. Consider a transnational corporation that has major operations in a country. If that country has strict regulations, the corporation's actions will be highly visible, and it may become an enforcement target if it flouts the law. At the same time, elephants are enormously strong and have all sorts of effects on the local ecosystem (potentially crushing trees, smaller animals, etc.). If a particular regulation angers an elephant, it may have the ability to change the rule.

The situation is quite different for mice, which are small, nimble, and multiply annoyingly quickly.[133] A good example on the Internet might be pornography sites. A profitable site can establish itself quickly, perhaps using bootlegged pictures that belong to other owners. If the site is shut down, the operator can

133. The metaphor of the mice was suggested in part by the "Stainless Steel Rat" series of novels by Harry Harrison. These novels, set in the future, describe the intelligent hero as a "stainless steel rat" who can move through the walls of high-technology society, violating the rules and evading capture.

simply open a new site, under a new name, and perhaps in a new jurisdiction. The same pictures might be back on the Internet the same day. Would-be regulators can run around furiously with a broom, but with little chance of getting rid of all the mice.

The metaphor of elephants and mice helps explain what sorts of sites are most subject to successful national regulation. Where the perceived harm is caused by elephants, the country has an especially good chance to stop the harm. By contrast, it will often be very difficult to stop perceived harms that are caused by mice. Inventors will keep trying to devise a better mousetrap, but with little hope of complete success. Drastic measures, such as using strong poisons, might get rid of the mice, but such poisons may also kill some freedoms that are cherished. A national ban on Internet access would stop the Internet harms, but it would also stop all of the good things the Internet can provide.

Applying the metaphor to privacy, large processors of information are the easiest elephants to identify. Examples include credit card companies, airline reservation systems, telephone companies, and the human resource databases of major companies. Even if they ship data to third countries, these firms typically have large operations in Europe and are clearly subject to enforcement actions there. Like elephants, these firms cannot hide—data protection authorities will be on the lookout for big databases that lack adequate protection. On the other hand, the elephants get undoubted advantages from their size. These sorts of companies can afford to participate in lobbying on the Directive and the implementing of national legislation. Like elephants, these companies also have a thick skin—they can defend themselves vigorously and can afford to pay fines if necessary.

This analysis suggests that national data protection rules might work reasonably effectively where the data is primarily in the hands of the largest companies. If few people outside of mainframe computer centers ever get access to the personal data, then that sort of data can be well protected. Similarly, we would expect the websites of elephants to comply relatively well with national laws and to install relatively strict privacy policies. Failure to do so will predictably lead to media and regulatory scrutiny.

At the other extreme, it will be extremely difficult for national regulators to effectively govern data processing by the mice of the electronic world. Many websites are run by individuals or small companies. A country may lack jurisdiction over the website. Even if jurisdiction can be established, there may be no effective way to identify or punish the wrongdoers. Individual users might reveal personal information to such a site, perhaps due to a fraudulent promise to keep information confidential or under the mistaken impression that the site will comply with data protection laws. As each crumb of information is received, the mouse might transfer the information to its favorite nest. Notably, databases filled with these crumbs might develop in countries that lack privacy laws.

The metaphor of elephants and mice applies similarly to other items on the

list above. Consider intellectual property. The elephants of the world will comply at a relatively high level with copyright laws and other requirements. Large companies, which do business in many countries, are subject to enforcement actions if they break the rules. If an elephant is doing something it should not, it can be very obvious. For instance, elephants that break copyright rules are subject to retaliation (and expensive damages) from any employee who becomes disgruntled and blows the whistle on the offending practice.[134] By contrast, mice might find stealing more profitable than paying for their food. For many owners of intellectual property, a crumb here or there is not worth the chase, especially when the chances of catching the pest are so slight.

This analysis of intellectual property is borne out in practice. For software, large companies routinely pay for site licenses while individual users are more likely to pass bootleg copies amongst themselves. The biggest threat to content providers is when their most valuable material is subject to easy copying by mice. Examples include music companies and Playboy Magazine, which sell primarily to individuals rather than large corporations that respect copyright rules. These content providers seem to be at risk of being nibbled to death by mice.[135] In response, these companies have taken vigorous action to close down websites that violate their copyrights and have appealed to users not to patronize sites that provide bootleg copies.[136]

What are countries to do when mice cause harm? Because it is so hard to find and catch the mice, the focus of legal regulation predictably falls on other groups, such as the users, Internet service providers, the payments system, or the offshore countries that shelter the mice. First, a country can punish users. For example, anyone caught gambling or accessing pornography can be punished. If a society has a strong enough consensus against the particular behavior, then punishing users may be legitimate. This approach does not work, however, for privacy issues. It makes no sense to punish persons for giving their own personal information to a website.

A second target can be the Internet Service Provider (ISP), who can be held liable if the allegedly harmful material is accessed through its service. ISPs are

134. There are other reasons why large companies may comply more with intellectual property rules than other companies. Large companies have in-house expertise in how to comply with such rules, and know how to get permission to use other companies' intellectual property. Large companies can afford to pay licensing fees. They also often own intellectual property of their own, and so have a vested interest in the system of property rules.

135. I take no position on whether such a death would be desirable for Playboy or any other content provider. I am simply describing the difficulty facing an owner of intellectual property that is subject to widespread copying by small websites that are accessible world-wide. On the problems facing producers of music CDs, *see* Jason Chervokas, *Internet CD Copying Tests Music Industry*, N.Y. TIMES, Apr. 6, 1998, at D3.

136. *See e.g.*, Playboy v. Webbworld, Inc., 968 F. Supp. 1171 (N.D. Tex. 1997); Playboy v. Russ Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997); Playboy v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993); Playboy v. Chuckleberry Publishing, Inc., 687 F.2d 563 (2d Cir. 1981).

firmly rooted in the customer's locality, and so are subject to jurisdiction and enforcement actions. Governments may thus find it overwhelmingly tempting to regulate ISPs. There are reasons, however, to be extremely cautious before instituting such regulation. Notably, harsh rules on ISPs may sharply increase the price and reduce the access to the many good things on the Internet. In addition, it is far from clear that ISPs have any effective ways to screen out bad content while permitting good content. The poison set for mice may also kill our favorite pets. And, even as the pets die off, new mice might emerge that are resistant to the poison. Search engines will let individuals find the hidden bad sites they seek. Mirror sites will let users get to bad sites that are supposedly banned by the ISP. And clever editing on the bad sites will let the prohibited words or pictures get through the ISP's filters (e.g., sites can take one letter out of vulgar words that trigger the ISP's filters). Over time, filtering technology may improve beyond its current crude state. Until it does, however, efforts to regulate at the ISP level will often be a nasty combination of being both overbroad and ineffective.

A third target for regulators can be the institutions that transfer money to the website operators. Some annoying mice give away information for free over the Web. Others, however, are vulnerable to the extent that regulators can stop the consumer from paying the website operator. Suppose, for instance, that it became illegal for a U.S. bank to transfer money on behalf of an individual, directly or indirectly, to a gambling operation outside of the United States. While great enforcement difficulties can be imagined, such a law illustrates how interruptions in financial flows might cut off sustenance to mice.[137]

A fourth target for regulators can be any offshore country that shelters the mice. The business opportunities of a mouse are constrained in a country where the activity is illegal—it is difficult and dangerous to become large and public enough to attract customers while remaining small and hidden enough to avoid the police. It is thus very tempting for mice to find a safe nest somewhere, such as in an offshore country. And, it is consequently tempting for the United States or other countries to exert pressure on the offshore haven. In the future, as a wide array of countries try to take advantage of global telecommunications to become offshore havens, we are likely to witness complex diplomatic maneuvers involving onshore and offshore countries.[138]

137. If such a law were passed, the gambling operations would presumably try to hide their identity, such as by having payment move through apparently "clean" front operations. Cutting off payments to the gambling operations would then closely parallel cutting off payments to drug cartels or others considered criminal by the onshore country. A chief goal of money laundering laws is to make it difficult to transfer funds to front operations. I am currently researching the interaction of money laundering laws, financial privacy, and the Internet.

138. For an illuminating discussion of tax havens and the countermeasures by fiscal authorities, *see* CAROLINE DOGGART, TAX HAVENS AND THEIR USES 113-34 (1997).

C. Elephants, Mice, and Choice of Law

The discussion here shows that legal regulation of Internet activity generally will be possible against elephants in the sense that elephants cannot hide easily and are usually subject to a country's jurisdiction. The possibility of enforcement against elephants does not imply that regulation will always occur. Constraints on regulation are likely as a matter of public choice theory, as the elephants use their bulk and strength to participate in the political process and oppose burdensome laws.[139] Constraints on enforcement will also come from elephants' thick hides, as they deploy legal counsel, public relations professionals, and other means to defend themselves in court and to otherwise discourage regulatory action.

The style of legal regulation will be different for mice. Where harms over the Internet are caused by mice, it will typically be difficult to identify the wrongdoers. Legal rules will obviously apply against mice in the few instances where the mice are actually caught. More often, however, regulation will focus on other parties—the individuals who do business with the mice, the ISPs that connect individuals to the mice, the payment intermediaries that transfer money to the mice, and the offshore countries that give the mice shelter. Precisely because mice can evade direct enforcement, nations will be tempted to try indirect enforcement.

The distinction between elephants and mice applies in a straightforward way to choice of law. Simply put, choice of law matters a great deal for elephants and usually not at all for mice. As defined here, elephants are large organizations that often have assets and economic activities spread widely across states and nations. When disputes arise, elephants will be subject to jurisdiction in various places. The key legal questions will then become ones of choice of law—out of the various jurisdictions that could apply their law to the elephant, which jurisdiction's rules will apply?

Where elephants sell to businesses, the choice of law rules will typically come from the Rome Convention, the CISG, and other existing sources of law. The more divisive questions will arise in the growing number of transactions directly between elephants and individual consumers. Within the United States[140] there is currently a contentious debate about choice of law rules in the proposed Uniform Commercial Code Article 2B. Many business interests wish to give the seller or licensor wide scope to select choice of law rules. In terms of the UCC debate, they support giving effect to the "shrinkwrap" or "clickwrap" licenses that

139. Under standard public choice theory, small, rich, and well-organized groups are likely to be especially effective in the political process. *See generally* Mancur Olson, The Logic of Collective Action (1965) (discussing advantages accruing to groups where a small number of actors receive the benefits of collective action).

140. Amelia H. Boss, *The Jurisdiction of Commercial Law: Party Autonomy in Choosing Applicable Law and Forum Under Proposed Revisions to the Uniform Commercial Code*, 32 Int'l Law. 1067 (1998).

are drafted by the licensor. In opposition, consumer advocates generally want individuals to be covered by their state consumer protection laws. Looking forward, one can predict similar debates at the international level. Large Internet merchants will wish to have transactions governed by the rules of a single forum, while individuals might expect to be protected by local consumer protection rules. For transactions involving elephants, therefore, one can foresee a major role for choice of law, both within the United States and internationally.

By contrast, choice of law will rarely be important for disputes arising from the behavior of mice. It will generally be difficult or impossible to identify the mice and bring them into court. Once identified, they will dispute jurisdiction. Once adjudged responsible, they will hide assets out of the reach of courts. With elephants, the problem is deciding which sovereign's rules will apply. With mice, the issue more often will be whether any sovereign's rules will be effective.[141]

IV. Conclusion

The initial task of this article was to explore some ways that choice of law would apply within the European Union and in transactions between the European Union and the United States. The existing system of choice of law in international transactions has largely concerned business-to-business transactions. Under the Rome Convention and other existing law, where multiple countries would have jurisdiction, businesses are given wide latitude to select the forum whose law will apply if disputes arise under a contract. Similar latitude is likely to exist for business-to-business transactions over the Internet.

The second task of the article was to examine the choice of law dimensions of the Data Protection Directive, which became effective in October 1998. The Data Protection Directive is especially relevant to the Internet because it seeks to regulate so many flows of data over the Internet. Its limit on transborder data flows is also an early example of the conflict that can arise as countries seek to restrict activities on one part of the Internet that are legal elsewhere.

In studying the Data Protection Directive, the article explained why article 4 should not be read as a grant of jurisdiction over websites in the United States and around the world. Study of the Data Protection Directive also helps reveal two important lessons for the international choice of law regime. First, the Directive shows both the attraction of harmonization as a way to eliminate choice of law problems and the limits of harmonization due to practical politics and the

141. There are circumstances where choice of law will matter to mice. Once an individual or small enterprise is identified and found to be within the jurisdiction of a country, that sovereign may indeed be able to apply civil or criminal penalties. An important choice of law problem can then exist where the activity was legal in one jurisdiction (such as for an offshore gambling casino) but was illegal in another jurisdiction (such as the onshore country). In such a situation, the onshore country will have to choose whether to apply its own or foreign law. At least where the activity is criminal in the onshore country, however, one might expect that country to select its own law.

persisting attractions of federalism and subsidiarity. Second, the Directive illustrates the relatively contained role for the courts in international choice of law compared to the large and growing role for transgovernmental networks of regulatory agencies who will often allocate national roles amongst themselves.

The third and most general task of this paper was to explore when legal regulation of the Internet will be effective. The nature of the Internet does not pose unique problems for enforcement against elephants. For the regulation of large corporations, the limits will be ones of political will to pass legislation and enforce it. By contrast, the nature of the Internet does pose new problems for the legal regulation of mice, who are difficult to find and often hide outside of the country. Because the Internet helps individuals conduct international transactions with unparalleled ease, the harms caused by these far-off mice are potentially large. Countries that cannot catch the mice themselves are thus tempted to enact laws regulating other parties, such as individual consumers, ISPs, payment providers, or other countries where the mice hide.

The metaphor of elephants and mice also instructs us on the future of international choice of law and the Internet. Elephants are often subject to jurisdiction in multiple countries. When disputes arise, the issue quickly becomes which sovereign's rules will apply—the classic choice of law question. As international sales to consumers become more prominent, choice of law disputes will often arise between the seller's country and the individual's national consumer protection law. On the other hand, the legal regulation of mice will more rarely implicate choice of law issues. The mice will disguise their identity, dispute jurisdiction, and hide their assets from judgment. Only rarely will they emerge into the light of open court to assert a defense based on choice of law.